Proof-of-Recourse Minting (PoRM) and Recourse-Backed Verified Assets (RBVA)

A Master Technical and Scientific Specification

Andrei Napoleonov
A5 MBL LTD, United Kingdom

December 26, 2025

Contents

Abstract **3**

1 Introduction and Problem Statement **3**

2 Accountability-First Paradigm **3**

3 Proof-of-Recourse Minting (PoRM) **3**

4 Recourse-Backed Verified Asset (RBVA) **4**

5 RBVA Lifecycle **4**

6 Economic Model **5**

7 Threat Model **5**

8 Regulatory and Legal Framework **5**

9 Governance and Evolution **6**

10 Conclusion **6**

A Appendix A: Formal Economic Model **6**
A.1 Agent Model 6
A.2 Utility Functions 6
A.3 Dominant Strategy Condition 7
A.4 Scalability of Attacks 7

B Appendix B: Threat Model **7**
B.1 Threat Classes 7
B.2 Security Assumptions 7
B.3 Security Conclusion 8

C Appendix C: Regulatory and Legal Mapping **8**
C.1 Howey Test (USA) 8
C.2 MiCA (EU) 8
C.3 UK FCA Classification 8

D Appendix D: Comparative Analysis **9**
D.1 Comparison with Existing Digital Assets 9
D.2 Key Differentiator 9

Abstract

I disclose a new paradigm for digital asset creation based on accountability-first principles. I introduce Proof-of-Recourse Minting (PoRM), a method in which digital assets may be issued only if a predefined, verifiable, and economically enforceable path of responsibility exists prior to issuance. Based on this method, I define a new class of digital assets, Recourse-Backed Verified Assets (RBVA), which embed obligation, evidence, and economic accountability as intrinsic properties. This document serves as a master specification, combining conceptual, economic, security, and regulatory analysis, and is intended to fix scientific and technical priority of the proposed approach.

1 Introduction and Problem Statement

Digital assets have achieved cryptographic security and global accessibility, yet they largely lack intrinsic accountability. Assets can be created without verified identity, enforceable obligation, or predefined consequences for misconduct. As a result, trust remains external, speculative, and fragile.

The core unresolved problem is the absence of responsibility as a prerequisite for digital asset existence.

2 Accountability-First Paradigm

I propose that accountability must precede issuance. Trust is treated not as a social expectation, but as an economically measurable and procedurally enforceable property.

> A digital asset should not exist if no valid path of responsibility exists.

This principle defines a new paradigm distinct from existing blockchain and token models.

3 Proof-of-Recourse Minting (PoRM)

PoRM is a method of digital asset issuance in which minting is permitted only after the following conditions are satisfied:

1. Binding to a verifiable identity;
2. Formalization of a concrete obligation;
3. Construction of a cryptographically anchored proof package;

4. Locking of an economic bond;

5. Predefinition of a recourse mechanism.

If any condition is not met, issuance is prohibited.

4 Recourse-Backed Verified Asset (RBVA)

An RBVA is a digital asset that simultaneously functions as:

- a representation of an obligation;
- a container of verifiable evidence;
- an economically bonded unit of responsibility.

RBVA is not money, not a security, and not an investment contract. It is an asset-obligation with enforceable accountability.

5 RBVA Lifecycle

RBVA progresses through the following states:

- CREATED
- ACTIVE
- DISPUTE_OPEN
- RESOLVED_NO_VIOLATION
- SLASHED
- RELEASED
- EXPIRED

Transitions are governed strictly by predefined rules and cannot be modified retroactively.

6 Economic Model

Let:

$$B = \text{bond size}, \quad S = \text{slashing fraction}, \quad G = \text{gain from violation}$$

The sufficient security condition is:

$$S \cdot B \geq \alpha \cdot G, \quad \alpha > 1$$

Under this condition, honest behavior dominates rational strategies.

RBVA liquidity is operational rather than speculative and derives from access and accountability requirements.

7 Threat Model

I analyze the following classes of attacks:

- Sybil and identity fraud;
- False obligation issuance;
- Non-performance attacks;
- Evidence tampering;
- Arbitration capture;
- Griefing and spam;
- Governance abuse.

All attacks are either prevented by design or rendered economically irrational.

8 Regulatory and Legal Framework

PoRM is a procedural method, not a financial product. RBVA does not promise profit, does not represent equity, and does not function as money.

Accordingly:

- RBVA does not satisfy the Howey Test;
- RBVA does not qualify as e-money or asset-referenced token under MiCA;
- RBVA aligns with utility and guarantee instruments under UK FCA guidance.

Compliance is achieved by architectural design rather than disclaimers.

9 Governance and Evolution

PoRM governance is bounded. Core invariants - identity binding, obligation, bond, and recourse - are immutable.

Policy parameters may evolve prospectively only, with explicit versioning and no retroactive effect.

10 Conclusion

I have presented a complete and self-contained specification of:

- a new paradigm for digital assets;
- a new issuance method (PoRM);
- a new asset class (RBVA);
- its economic, security, and legal foundations.

This work establishes scientific and technical priority and provides a foundation for implementation, standardization, and further research.

A Appendix A: Formal Economic Model

This appendix provides a formal economic justification of the Proof-of-Recourse Minting (PoRM) method.

A.1 Agent Model

We consider rational agents maximizing expected utility:

- Issuer (I)
- Counterparty (C)
- Adversary (A)

A.2 Utility Functions

Honest behavior:

$$U_H = V + U - C_{op}$$

Dishonest behavior:

$$U_A = G - p_d(S \cdot B + C_{arb} + R)$$

A.3 Dominant Strategy Condition

Honesty dominates if:

$$U_H > U_A$$

Which yields:

$$S \cdot B \geq \alpha \cdot G, \quad \alpha > 1$$

This condition ensures economic security by design.

A.4 Scalability of Attacks

For k parallel attacks:

$$C_{attack}(k) = k(S \cdot B)$$

Since gain scales linearly, attacks are not economically scalable.

B Appendix B: Threat Model

This appendix formalizes the threat landscape for PoRM and RBVA.

B.1 Threat Classes

We identify the following threat categories:

1. Sybil and identity fraud
2. False obligation issuance
3. Non-performance attacks
4. Evidence tampering
5. Arbitration capture
6. Griefing and spam
7. Governance manipulation

B.2 Security Assumptions

The system assumes:

- rational adversaries;
- bounded economic resources;

- verifiable identity mechanisms;
- cryptographic integrity of proofs.

B.3 Security Conclusion

All identified threats are either:

- prevented structurally, or
- rendered economically irrational.

C Appendix C: Regulatory and Legal Mapping

This appendix provides a comparative legal analysis of RBVA.

C.1 Howey Test (USA)

RBVA fails to satisfy the four elements of the Howey Test:

- no investment of money;
- no common enterprise;
- no expectation of profit;
- no reliance on efforts of others.

C.2 MiCA (EU)

RBVA does not qualify as:

- asset-referenced token;
- e-money token.

RBVA is best classified as a utility and guarantee crypto-asset.

C.3 UK FCA Classification

RBVA aligns with unregulated utility tokens under FCA guidance, subject to disclosure.

D Appendix D: Comparative Analysis

D.1 Comparison with Existing Digital Assets

Feature	Token	NFT	Stablecoin	RBVA
Obligation	No	No	Partial	Yes
Bond	No	No	Reserve	Yes
Recourse	No	No	Limited	Yes
Accountability	No	No	Issuer	Economic
Operational Liquidity	No	No	Limited	Yes

D.2 Key Differentiator

RBVA is the only digital asset class that requires enforceable accountability *prior to existence*.